Secrecy Cooperative Networks with Outdated Relay Selection over Correlated Fading Channels

Impact of Correlated Fading Channels on Multiple Secure Relaying with Outdated Relay Selection

Lisheng Fan, Xianfu Lei, Nan Yang, *Member, IEEE*, Trung Q. Duong, *Senior Member, IEEE*, and George K. Karagiannidis, *Fellow, IEEE*

***Abstract*—In this paper, we study the impact of correlated fading channels on multiple secure decode-and-forward (DF) relaying with outdated relay selection, where the information transmission assisted by the N DF relays from the source to the destination can be overheard by the eavesdropper in the network. The eavesdropping channels are correlated with the main channels, which affects the network security. To enhance the network security, one best relay is chosen to assist the secure transmission, which is however maybe outdated in time-varying channel environments. The impact of both channel correlation and outdated relay selection on the secrecy performance is studied by deriving the analytical expression of the secrecy outage probability (SOP). The asymptotic SOP is also provided with high main-to-eavesdropper ratio (MER). From the asymptotic SOP, we find that only the outdated degree of relay selection affects the network secrecy diversity order, but the channel correlation does not. Moreover, it is interesting to find that the channel correlation is beneficial to the transmission security in the high MER regime.**

***Index Terms*—Secure communications, correlated fading channels, outdated relay selection, secrecy diversity order.**

I. Introduction

Due to the broadcast nature, the wireless transmission may be overheard by eavesdroppers in the network, and the severe issue of information leakage arises [1]. To prevent the wiretap, the encryption algorithm and physical-layer security (PLS) have been studied in the literature. The pioneering work of PLS is investigated by Wyner [2], where the wiretap channel model was firstly proposed. Then researchers extended to fading channels and studies the important metrics of secrecy performance, such as secrecy capacity and secrecy outage probability (SOP) [3]–[5]. As relaying is a promising technique for the next-generation communications, it is of vital importance to investigate the PLS of relay networks. For amplify-and-forward (AF) and decode-and-forward (DF) relaying, the secrecy performance has been studied by deriving the analytical expression of SOP [6]–[8]. Moreover, the asymptotic SOP with high main-to-eavesdropper ratio (MER) was provided to obtain the insights on the system.

L. Fan is with the School of Computer Science and Educational Software, Guangzhou University, Guangzhou, China (e-mail: lsfan_gzu@126.com).

X. Lei is with the Provincial Key Lab of Information Coding and Transmission, Southwest Jiaotong University, Chengdu, China (e-mail: xflei@home.swjtu.edu.cn).

N. Yang is with Australian National University, Canberra ACT 0200, Australia (e-mail: yangnan1616@gmail.com).

T. Q. Duong is with Queen's University Belfast, Belfast BT7 1NN, United Kingdom (e-mail: trung.q.duong@qub.ac.uk).

G. K. Karagiannidis is with Aristotle University of Thessaloniki, Thessaloniki 54 124, Greece (e-mail: geokarag@auth.gr).

Manuscript received XXX, XX, 2016; revised XXX, XX, 2016.

In the most existing works of the literature, the eavesdropping channels are assumed to be independent of the main channels. However, this ideal assumption may not hold in practice due to many factors such as antenna deployments, proximity of the legitimate receiver and eavesdropper, and scattering environments. The impact of channel correlation between the main and eavesdropping links on the secrecy performance is studied in [9], [10], where it has been found that the channel correlation is harmful to the transmission security in the low MER region. To enhance the transmission security, the opportunistic selection is an effective technique to exploit the channel fluctuation between antennas, users and relays [7], [11]. The selection can be implemented in a centralized or distributed manner through dedicated feedback links, which may take some time to complete. In time-varying channel environments, the channels may vary from the instant of selection to that of actual data transmission, which causes the selection based on the outdated channel state information (CSI) [12] and severely limits the system secrecy performance [13], [14].

In this paper, we investigate the secure multi-relay networks with channel correlation between the main and eavesdropping links, where the information transmission assisted by N DF relays from the source to the destination may be overheard by the eavesdropper in the network. To strengthen the secure transmission, one best relay is selected among N relays, which is however based on the outdated CSI in time-varying channel environments. We study the impact of both channel correlation and outdated relay selection by deriving the analytical and asymptotic expressions for the SOP. From the asymptotic result, we find that the secrecy diversity order is equal to N only in perfect channel state information; otherwise it degenerates to unity. Moreover, the channel correlation does not affect the secrecy diversity order, but it can help strength the secure transmission in high MER region.

Notations: The notation $\mathcal{CN}(0,\sigma^2)$ denotes a circularly symmetric complex Gaussian random variable (RV) with zero mean and variance σ^2. We use $f_X(\cdot)$ to represent the probability density function (PDF) of the RV X. In addition, $I_0(x)$ is the modified Bessel function of the first kind of order zero [15], $\Pr[\cdot]$ returns the probability, and $E[\cdot]$ denotes the statistical average. We use $h_{A,B}$ to denote the channel parameter of the A–B link.

II. System Model

Fig. 1 shows the system model of a two-phase secure multiple DF relays network, where the information transmission

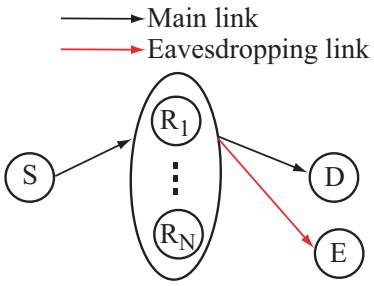

Fig. 1. A two-phase secure multiple DF relaying network.

from the source S to the destination D can be overheard by the eavesdropper E. There are no direct links from S to D and E, and the information transmission are only through the N relays $\{R_n|1 \leq n \leq N\}$. One best relay is chosen among N available relays to assist the secure transmission. However, the selection may be outdated in time-varying channel environments, and the best relay is not always chosen. In addition, due to the reasons such as antenna deployment and radio scattering, the channels at the receivers D and E are correlated with each other, i.e., $h_{R_n,D}$ is correlated with $h_{R_n,E}$. Due to the size limitation, the nodes in the network are equipped with a single antenna, and all links experience time-varying Rayleigh fading. In the following, we present the two-phase secure data transmission process and the relay selection criterion for the considered system.

Suppose that the relay R_n is used for the two-phase secure data transmission. In the first phase, the source S sends signal x_S to R_n with transmit power P, and R_n receives,

$$y_{R_n} = \sqrt{P} h_{S,R_n} x_S + n_{R_n}, \tag{1}$$

where $h_{S,R_n} \sim \mathcal{CN}(0,\alpha)$ denotes the channel parameter of the S–R_n link, and $n_{R_n} \sim \mathcal{CN}(0,\sigma^2)$ is the additive white Gaussian noise (AWGN) at the relay R_n. If the relay R_n can correctly decode the message from the source, i.e., it can support a target data rate R_t,

$$\frac{1}{2}\log_2\left(1+\frac{P|h_{S,R_n}|^2}{\sigma^2}\right) \geq R_t, \tag{2}$$

the relay forwards the message to D in the second phase with the transmit power P. Accordingly, D and E receive,

$$y_D = \sqrt{P} h_{R_n,D} x_S + n_D, \tag{3}$$

$$y_E = \sqrt{P} h_{R_n,E} x_S + n_E, \tag{4}$$

where $h_{R_n,D} \sim \mathcal{CN}(0,\beta)$ and $h_{R_n,E} \sim \mathcal{CN}(0,\varepsilon)$ are the channel parameters of the R_n–D and R_n–E links, respectively. The noise terms $n_D \sim \mathcal{CN}(0,\sigma^2)$ and $n_E \sim \mathcal{CN}(0,\sigma^2)$ are the AWGN at D and E, respectively.

We use $u_n = |h_{S,R_n}|^2$, $v_n = |h_{R_n,D}|^2$ and $w_n = |h_{R_n,E}|^2$ to represent the channel gains of the S–R_n, R_n–D and R_n–E links, respectively. The secrecy outage occurs when the data rate difference between the main and eavesdropping links falls below a target secrecy data rate R_s,

$$\frac{1}{2}\log_2\left(1+\frac{P}{\sigma^2}v_n\right) - \frac{1}{2}\log_2\left(1+\frac{P}{\sigma^2}w_n\right) < R_s, \tag{5}$$

which is equivalent to

$$\frac{1+\tilde{P}v_n}{1+\tilde{P}w_n} < \gamma_s, \tag{6}$$

where $\tilde{P} = P/\sigma^2$ denotes the transmit SNR, and $\gamma_s = 2^{2R_s}$ is the secrecy SNR threshold.

To enhance the transmission security, we need to select one best relay to strength the secure data transmission. Let Ω denote the candidate set of relays that can successfully decode the message from the source. Then based on the main channels only[1], the relay selection is performed to choose one best relay R_{n^*} among Ω,

$$n^* = \arg\max_{n\in\Omega} v_n, \tag{7}$$

which maximizes the received SNR at the destination D.

III. Channel Correlation and Outdated Relay Selection

In this work, we consider the correlated channels between the receivers D and E, and the correlation between v_n and w_n is characterized by [10]

$$f_{w_n|v_n}(w|v) = \frac{I_0\left(\frac{2}{1-\rho_c}\sqrt{\frac{\rho_c v w}{\beta\epsilon}}\right)}{(1-\rho_c)\beta\varepsilon} e^{-\frac{\frac{\rho_c v}{\beta}+\frac{w}{\varepsilon}}{1-\rho_c}}, \tag{8}$$

where $\rho_c \in [0,1]$ is the power correlation coefficient. Specifically, $\rho_c = 0$ represents that v_n is independent of w_n, while $\rho_c = 1$ denotes the completely linear correlation.

Besides the channel correlation, the outdated relay selection has a significant impact on the network security. The selection of (7) can be implemented in a distributed or centralized manner in practice, through some dedicated feedback channels [7]. However, due to the limited feedback resources, the channels may vary from the instant of relay selection to that of actual data transmission in time-varying channel environments. Let $\tilde{v}_{n^*}$ and v_{n^*} denote the channels of R_{n^*}–D at the instants of relay selection and actual data transmission, respectively. The outdated selection can be characterized by the conditional PDF $f_{v_{n^*}|\tilde{v}_{n^*}}(v|\tilde{v})$ [12],

$$f_{v_{n^*}|\tilde{v}_{n^*}}(v|\tilde{v}) = \frac{1}{(1-\rho_o)\beta} e^{-\frac{\rho_o\tilde{v}+v}{(1-\rho_o)\beta}} I_0\left(\frac{2\sqrt{\rho_o v\tilde{v}}}{(1-\rho_o)\beta}\right), \tag{9}$$

where $\rho_o \in [0,1]$ denotes the outdated degree of relay selection. In particular, $\rho_o = 1$ denotes that the selection is based on the perfect CSI, while $\rho_o = 0$ represents the completely outdated relay selection.

In the following, we will study the impact of channel correlation and outdated relay selection on the network secrecy performance by providing the analytical and asymptotic expressions of secrecy outage probability.

[1]The instantaneous channel parameters of eavesdropping links are not involved in the relay selection criterion, since they are generally hard to obtain in practice.

$$\mathcal{P}_{out} = \sum_{K=1}^{N} \binom{N}{K} e^{-\frac{K\gamma_t}{\tilde{P}\alpha}} \left(1 - e^{-\frac{\gamma_t}{\tilde{P}\alpha}}\right)^{N-K} \left(1 - \sum_{k=1}^{K} \sum_{m=0}^{T} \sum_{i=0}^{m} \sum_{j=0}^{i} C_{km} d_{m,ij} (m+j)! (b_1\gamma_s + b_2)^{-(m+j+1)}\right). \quad (25)$$

IV. Secrecy Outage Probability

A. Analytical Expression

Note that the set Ω may have $K (K = 1, 2, \cdots, N)$ candidates that can correctly decode the message from the source, we can express the SOP of the considered system as

$$\mathcal{P}_{out} = \sum_{K=1}^{N} \binom{N}{K} \Pr\Big[\tilde{P}u_1 \geq \gamma_t, \cdots, \tilde{P}u_K \geq \gamma_t, \tilde{P}u_{K+1} < \gamma_t, \cdots, \tilde{P}u_N < \gamma_t, \frac{1+\tilde{P}v_{n^*}}{1+\tilde{P}w_{n^*}} < \gamma_s\Big], \quad (10)$$

where $\gamma_t = 2^{2R_t} - 1$ denotes the SNR threshold of successful decoding at the relay. Since the random variable u_n is independent of v_{n^*} and w_{n^*}, we can rewrite $\mathcal{P}_{out}$ as

$$\mathcal{P}_{out} = \sum_{K=1}^{N} \binom{N}{K} \Pr\Big[\tilde{P}u_1 \geq \gamma_t, \cdots, \tilde{P}u_K \geq \gamma_t, \tilde{P}u_{K+1} < \gamma_t, \cdots, \tilde{P}u_N < \gamma_t\Big] \Pr\Big[\frac{1+\tilde{P}v_{n^*}}{1+\tilde{P}w_{n^*}} < \gamma_s\Big] \quad (11)$$

$$= \sum_{K=1}^{N} \binom{N}{K} e^{-\frac{K\gamma_t}{\tilde{P}\alpha}} \left(1 - e^{-\frac{\gamma_t}{\tilde{P}\alpha}}\right)^{N-K} \underbrace{\Pr\Big[\frac{1+\tilde{P}v_{n^*}}{1+\tilde{P}w_{n^*}} < \gamma_s\Big]}_{J_K}, \quad (12)$$

where the PDF of $f_{u_n}(u) = \frac{1}{\alpha} e^{-\frac{u}{\alpha}}$ is applied and the probability J_K denotes the conditional SOP with the given K active relays. From the selection criterion in (7) and the conditional PDF of $f_{v_{n^*}|\tilde{v}_{n^*}}(v|\tilde{v})$ in (9), the PDF of v_{n^*} is given by [12]

$$f_{v_{n^*}}(v) = \sum_{k=1}^{K} \binom{K}{k} \frac{k(-1)^{k-1}}{\beta[k(1-\rho_o)+\rho_o]} e^{-\frac{kv}{[k(1-\rho_o)+\rho_o]\beta}}. \quad (13)$$

From the above $f_{v_{n^*}}(v)$ and the conditional $f_{w_n|v_n}(w|v)$ in (8), we obtain the joint PDF of v_{n^*} and w_{n^*} as,

$$f_{v_{n^*},w_{n^*}}(v,w) = f_{w_{n^*}|v_{n^*}}(w|v) f_{v_{n^*}}(v)$$
$$= \sum_{k=1}^{K} \binom{K}{k} \frac{k(-1)^{k-1}}{\beta\varepsilon(1-\rho_c)[k(1-\rho_o)+\rho_o]} I_0\Big(\frac{2}{1-\rho_c}\sqrt{\frac{\rho_c v w}{\beta\varepsilon}}\Big) \times e^{-\frac{kv}{[k(1-\rho_o)+\rho_o]\beta} - (\frac{\rho_c v}{\beta} + \frac{w}{\varepsilon})\frac{1}{1-\rho_c}}. \quad (14)$$

Note that the Bessel function $I_0(x)$ can be expanded by the series as [15]

$$I_0(x) = \sum_{m=0}^{\infty} \frac{x^{2m}}{4^m (m!)^2} \quad (15)$$

$$\approx \sum_{m=0}^{T} \frac{x^{2m}}{4^m (m!)^2}, \quad (16)$$

where the truncation error in (16) decays exponentially with T [10]. Hence with an efficient number of series, we can obtain an accurate approximation for $I_0(x)$. In the following, we ignore the approximation error, and re-express $f_{v_{n^*},w_{n^*}}(v,w)$ as

$$f_{v_{n^*},w_{n^*}}(v,w) = \sum_{k=1}^{K} \sum_{m=0}^{T} C_{km} v^m w^m e^{-b_1 v} e^{-b_2 w}, \quad (17)$$

with

$$C_{km} = \binom{K}{k} \frac{k(-1)^{k-1}}{k(1-\rho_o)+\rho_o} \frac{\rho_c^m}{(1-\rho_c)^{2m+1}(\beta\varepsilon)^{m+1}(m!)^2}, \quad (18)$$

$$b_1 = \Big(\frac{k}{k(1-\rho_o)+\rho_o} + \frac{\rho_c}{1-\rho_c}\Big)\frac{1}{\beta}, \quad (19)$$

$$b_2 = \frac{1}{(1-\rho_c)\varepsilon}. \quad (20)$$

From (17), we can compute J_K as

$$J_K = \Pr\big(v_{n^*} < \frac{\gamma_s - 1}{\tilde{P}} + \gamma_s w_{n^*}\big) \quad (21)$$

$$= \int_0^{\infty} \int_0^{\frac{\gamma_s-1}{\tilde{P}} + \gamma_s w} f_{v_{n^*},w_{n^*}}(v,w) dv dw \quad (22)$$

$$= 1 - \sum_{k=1}^{K} \sum_{m=0}^{T} \sum_{i=0}^{m} \sum_{j=0}^{i} C_{km} d_{m,ij} (m+j)! \times (b_1\gamma_s + b_2)^{-(m+j+1)}, \quad (23)$$

with

$$d_{m,ij} = \frac{m!}{i!}\binom{i}{j} \frac{e^{-b_1(\gamma_s-1)/\tilde{P}}}{b_1^{m-i+1}} \gamma_s^j \big(\frac{\gamma_s - 1}{\tilde{P}}\big)^{i-j}. \quad (24)$$

By applying the result of J_K into (12), we can obtain the analytical SOP for the multiple secure relaying with channel correlation and outdated relay selection, as shown in (25) at the top of this page. Note that the obtained analytical SOP consists of elementary functions only, and hence is easily to be evaluated.

B. Asymptotic Expression

To obtain the insights on the system, we now extend to derive the asymptotic SOP with high MER. With a large transmit power P, we can approximate $\mathcal{P}_{out}$ as

$$\mathcal{P}_{out} \simeq J_N \quad (26)$$

$$\simeq \Pr\big(\frac{v_{n^*}}{w_{n^*}} < \gamma_s\big). \quad (27)$$

Let $z = \frac{v_{n^*}}{w_{n^*}}$, and then the PDF of z is derived as

$$f_z(z) = \int_0^\infty w f_{v_{n^*},w_{n^*}}(wz, w)dw \tag{28}$$

$$= \sum_{k=1}^{N} \binom{N}{k} \frac{k(-1)^{k-1}}{\beta\varepsilon(1-\rho_c)[k(1-\rho_o)+\rho_o]} \times \frac{\frac{kz}{[k(1-\rho_o)+\rho_o]\beta} + \left(\frac{\rho_c z}{\beta} + \frac{1}{\varepsilon}\right)\frac{1}{1-\rho_c}}{\left[\left(\frac{kz}{[k(1-\rho_o)+\rho_o]\beta} + \left(\frac{\rho_c z}{\beta} + \frac{1}{\varepsilon}\right)\frac{1}{1-\rho_c}\right)^2 - \frac{4\rho_c z}{(1-\rho_c)^2\beta\varepsilon}\right]^{3/2}}, \tag{29}$$

where [15, eq. (6.623.2)] is applied in the last equality. For high MER with $\beta \gg \varepsilon$, we can approximate $f_z(z)$ as

$$f_z(z) \simeq \sum_{k=1}^{N} \binom{N}{k} \frac{(-1)^{k-1}(1-\rho_c)\lambda[k(1-\rho_o)+\rho_o]}{\{\lambda + k(1-\rho_c)z + \rho_c z[k(1-\rho_o)+\rho_o]\}^2}, \tag{30}$$

where $\lambda = \beta/\varepsilon$ is the MER. From the above $f_z(z)$, we then approximate $\mathcal{P}_{out}$ as

$$\mathcal{P}_{out} \simeq \int_0^{\gamma_s} f_z(z)dz \tag{31}$$

$$\simeq \begin{cases} N!\left(\frac{(1-\rho_c)\gamma_s}{\lambda}\right)^N, & \text{If } \rho_o = 1 \\ \frac{(1-\rho_c)\gamma_s}{\lambda}\left(\sum_{k=1}^{N}\binom{N}{k}\frac{k(-1)^{k-1}}{k(1-\rho_o)+\rho_o}\right), & \text{If } \rho_o < 1 \end{cases} \tag{32}$$

where we apply the approximation of $(1+x)^{-1} = \sum_{k=0}^{N}(-1)^k x^k$ [15] from (31) to (32). From this asymptotic result, we have the following remarks on the network security:

Remark 1: For a given number of relays, the network secrecy diversity order depends on the outdated degree of relay selection, but not on the channel correlation.

Remark 2: The network secrecy diversity order is equal to N when $\rho_o = 1$, indicating that the network security can be rapidly enhanced by increasing the number of relays in the perfect CSI environments.

Remark 3: As long as the relay selection is outdated, the network secrecy diversity order degenerates to unity. This is because there exists a possible wrong relay selection with an outdated CSI. This incorrect selection limits the entire network secrecy performance.

Remark 4: The channel correlation between the main and eavesdropping channels is beneficial to the transmission security in high MER region[2]. With higher channel correlation, the destination has more information about the channel fluctuation of eavesdropping links. In particular, for the completely linear correlation with $\rho_c = 1$, the fluctuation of eavesdropping channels is completely accordance with that of main channels and hence the destination has the perfect information about the channel fluctuation of eavesdropping links, making v_{n^*}/w_{n^*} equal to β/ε. This helps the network suppress the wiretap perfectly, leading to a zero SOP.

[2]Note that in the low MER region, the channel correlation is however harmful to the secure transmission [9], [10].

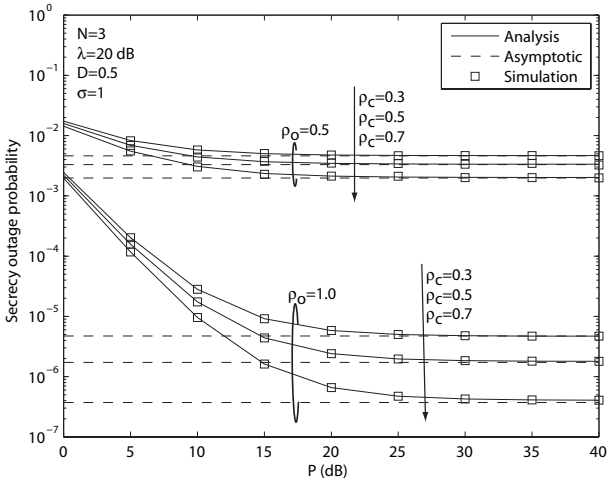

Fig. 2. Secrecy outage probability versus the transmit power P.

V. Numerical and Simulation Results

In this section, we provide some numerical and simulation results to verify the proposed studies for the multiple secure relaying with channel correlation and outdated relay selection. All links in the network experience Rayleigh fading, and we adopt the path-loss model with exponent of four to measure the average channel gains of main links. Without loss of generality, we normalize the distance between the source and destination to unity, where the relays are in between of them. Let D denote the distance between the source and relays, and accordingly, $\alpha = D^{-4}$ and $\beta = (1-D)^{-4}$ are set. The target data rate R_t of the first hop is 1 bps/Hz, and hence the associated γ_t is 3. The secrecy data rate R_s is 0.2 bps/Hz, so that the secrecy SNR threshold γ_s is 1.32.

Fig. 2 demonstrates the numerical and simulated secrecy outage probabilities versus the transmit power P, where $N = 3$, $\lambda = 20$dB and $D = 0.5$. Several cases of channel correlation are considered with $\rho_c = 0.3$, 0.5 and 0.7. Both perfect and outdated CSI environments are studied with $\rho_o = 1.0$ and 0.5, respectively. As observed from the figure, for different values of ρ_c and ρ_o, the analytical result matches well with the simulation one, and the asymptotic result converges to the exact one when P is large. This validates the derived analytical and asymptotic expressions of the SOP. Moreover, in both perfect and outdated CSI environments, the secrecy performance becomes better with larger ρ_c, as higher channel correlation helps the destination have more information about the channel fluctuation of eavesdropping links. The secrecy performance also improves with larger ρ_o, as better CSI helps select the best relay to assist the secure transmission. Furthermore, the secrecy performance improves with larger P. But the improvement is saturated in high P region, as the fixed MER becomes the bottleneck of the secrecy performance.

Fig. 3 illustrates the secrecy outage probability versus MER with different values of ρ_c and ρ_o, where $P = 40$dB and N varies from 1 to 3. We can see from this figure that for different values of N, ρ_c and ρ_o, the analytical result fits well with the simulation one, and the asymptotic result converges to the simulation one in the high MER region. Moreover,

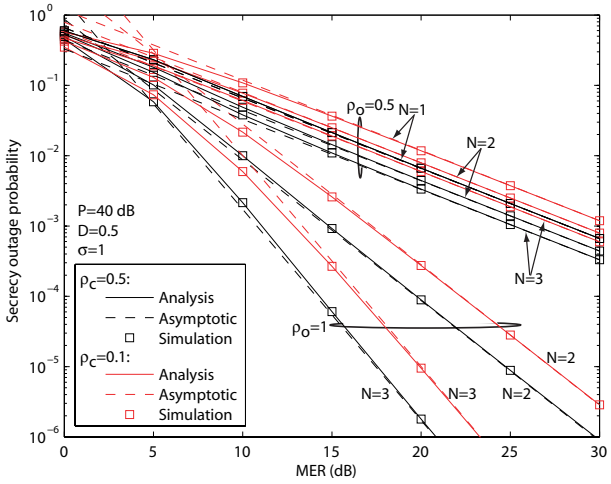

Fig. 3. Secrecy outage probability versus MER.

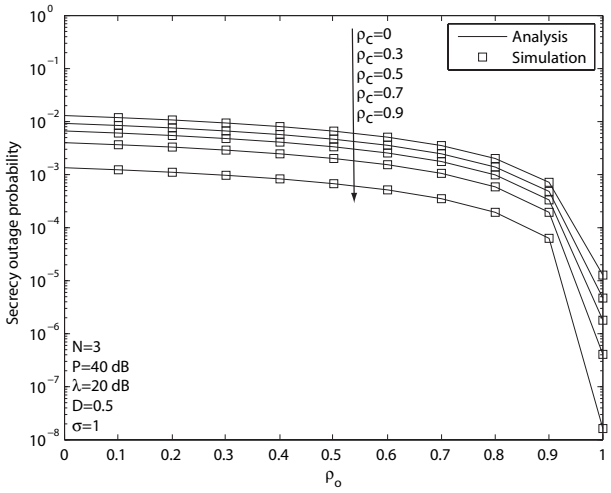

Fig. 4. Impact of ρ_c and ρ_o on the secrecy outage probability.

only the value of ρ_o affects the curve slopes, but ρ_c does not. This indicates that the secrecy diversity order depends on the outdated degree of relay selection, but not on the channel correlation. In particular, the curves are in parallel with each other for different relay numbers when $\rho_o = 0.5$, indicating that the system secrecy diversity order is unity for different values of ρ_c as long as the selection is outdated. On the contrast, the curve slope is proportional to N in the perfect CSI with $\rho_o = 1$, indicating that the system full secrecy diversity order can be achieved for different values of ρ_c. Such observations validate the insights from the asymptotic expression of the SOP.

Fig. 4 depicts the impact of ρ_c and ρ_o on the secrecy outage probability with $N = 3$ and $\lambda = 20$dB, where ρ_o ranges from 0 to 1 and ρ_c varies in $\{0, 0.3, 0.5, 0.7, 0.9\}$. We can find that for different values of ρ_c and ρ_o, the analytical result matches well with the simulation one. Moreover, the secrecy performance improves with larger ρ_c and ρ_o. This is because that higher channel correlation helps the destination have more information about the channel fluctuation of eavesdropping links, and better CSI helps select the best relay to assist the secure transmission.

VI. Conclusion

In this paper, we investigated the secure relaying with N DF relays, where the main and eavesdropping channels are correlated. The relay selection was performed to choose one best relay to assist the secure transmission, which is however maybe outdated. We studied the impact of channel correlation and outdated relay selection on the secrecy performance by deriving the analytical SOP as well as the asymptotic expression with high MER. From the asymptotic SOP, we found that the channel correlation does not affect the secrecy diversity order, but can be beneficial to the transmission security. Importantly, we confirmed that the full secrecy diversity order of N is achieved only when the selection is based on the perfect CSI.

References

[1] N. Yang, L. Wang, G. Geraci, M. Elkashlan, J. Yuan, and M. D. Renzo, "Safeguarding 5G wireless communication networks using physical layer security," *IEEE Commun. Mag.*, vol. 53, no. 4, pp. 20–27, Apr. 2015.

[2] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1367, Oct. 1975.

[3] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information theoretic security," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515–2534, Jun. 2008.

[4] P. K. Gopala, L. Lai, and H. E. Gamal, "On the secrecy capacity of fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 10, pp. 4687–4698, Oct. 2008.

[5] M. Z. I. Sarkar and T. Ratnarajah, "Secure communication through Nakagami-m fading MISO channel," in *IEEE Inter. Conf. on Commun. (ICC)*, Kyoto, Japan, 2011.

[6] Y. Zou, X. Wang, and W. Shen, "Optimal relay selection for physical-layer security in cooperative wireless networks," *IEEE J. Select. Areas Commun.*, vol. 31, no. 10, pp. 2099–2111, Oct. 2013.

[7] L. Fan, X. Lei, T. Q. Duong, M. Elkashlan, and G. K. Karagiannidis, "Secure multiuser communications in multiple amplify-and-forward relay networks," *IEEE Trans. Commun.*, vol. 62, no. 9, pp. 3299–3310, Sept. 2014.

[8] J. Mo, M. Tao, and Y. Liu, "Relay placement for physical layer security: A secure connection perspective," *IEEE Commun. Lett.*, vol. 16, no. 6, pp. 878–881, Jun. 2012.

[9] H. Jeon, N. Kim, J. Choi, H. Lee, and J. Ha, "Bounds on secrecy capacity over correlated ergodic fading channels at high SNR," *IEEE Trans. Inf. Theory*, vol. 57, no. 4, pp. 4005–4019, Apr. 2011.

[10] X. Sun, J. Wang, W. Xu, and C. Zhao, "Performance of secure communications over correlated fading channels," *IEEE Sig. Proc. Lett.*, vol. 19, no. 8, pp. 479–482, Aug. 2012.

[11] N. Yang, P. L. Yeoh, M. Elkashlan, R. Schober, and J. Yuan, "MIMO wiretap channels: Secure transmission using transmit antenna selection and receive generalized selection combining," *IEEE Commun. Lett.*, vol. 17, no. 9, pp. 1754–1757, Sept. 2013.

[12] M. Torabi and D. Haccoun, "Capacity analysis of opportunistic relaying in cooperative systems with outdated channel information," *IEEE Commun. Lett.*, vol. 14, no. 12, pp. 1137–1139, Dec. 2010.

[13] N. S. Ferdinand, D. B. da Costa, and M. Latva-aho, "Effects of outdated CSI on the secrecy performance of MISO wiretap channels with transmit antenna selection," *IEEE Commun. Lett.*, vol. 17, no. 5, pp. 864–867, May 2013.

[14] Y. Huang, F. S. Al-Qahtani, T. Q. Duong, and J. Wang, "Secure transmission in MIMO wiretap channels using general-order transmit antenna selection with outdated CSI," *IEEE Trans. Commun.*, vol. 63, no. 8, pp. 2959–2971, Aug. 2015.

[15] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series, and Products*, 7th ed. San Diego, CA: Academic, 2007.